Mahesh Sreekumar Rajasree[1,2]

Assistant Professor, University of Warsaw
Institute of Informatics
Faculty of Mathematics, Informatics and Mechanics
Warsaw, Poland

PRINCIPAL INTERESTS Cryptography, Quantum Cryptography, Lattice theory, Algorithms, Cryptanalysis

Employment

Assistant Professor October 2026 - Present
Institute of Informatics
Faculty of Mathematics, Informatics and Mechanics
University of Warsaw, Warsaw, Poland

Postdoctoral Researcher December 2024 - September 2026
Host: Prof. Nico Döttling
CISPA Helmholtz Center for Information Security
Saarbrücken, Saarland, Germany

Postdoctoral Fellow April 2023 - November 2024
Supervisor: Prof. Venkata Koppula
Computer Science and Engineering
Indian Institute of Technology Delhi, New Delhi, India

ACADEMIC BACKGROUND

Ph.D. & M.Tech. Computer Science and Engineering August 2016 - July 2023
Indian Institute of Technology Kanpur, Uttar Pradesh, India

- Advisor: Prof. Manindra Agrawal
- Ph.D. Thesis: Analysis of Symmetric-Key Cryptosystems and Subset-Sum Problem
- M.Tech. Thesis: New Results and Proofs in Lattice Theory
- CPI: 10/10

B.Tech. Computer Science and Engineering August 2012 - May 2016
National Institute of Technology Calicut, Kerala, India

- Advisor: Dr. Sumesh T.A.
- B.Tech. Thesis: Firewall for Preventing Anonymous Proxy Usage
- CPI: 8.89/10

Secondary & Higher Secondary Education June 2009 - March 2012
Arya Central School, Trivandrum, Kerala, India

- All India Senior Secondary School Examination Percentage: 91.2
- All India Secondary School Examination CGPA: 9.6/10

Peer-reviewed Works

1. **On Robust Combiners for Pseudorandom Codes and PKE with Pseudorandom Ciphertexts**
   with Nico Döttling, Venkata Koppula and Felix Rohrbach
   Theory of Cryptography Conference, TCC 2026

[1] maheshsr@mimuw.edu.pl
[2] https://mahe94.github.io

2. **Pigeonhole Equal Subset Sum: Subexponential Algorithm, Tight Lower Bounds and Average-Case Analysis**
   with Deepak Bhati, Pranjal Dutta, Antoine Joux and Karol Węgrzycki
   67th Annual Symposium on Foundations of Computer Science, FOCS 2026
3. **Chosen Ciphertext Secure Pseudorandom Codes in the Standard Model**
   with Nico Döttling, Antoine Joux, Venkata Koppula and Hendrik Waldner
   46th Annual International Cryptology Conference, CRYPTO 2026
4. **Separating Pseudorandom Codes from Local Oracles**
   with Nico Döttling and Anne Müller
   23rd Theory of Cryptography, TCC 2025
   Outstanding Paper Award
5. **Incompressible Encryption Beyond CPA/CCA Security**
   with Venkata Koppula, Abhinav Kumar and Harihar Swaminathan
   IACR Communications in Cryptology, Volume 2, Issue 2, Article 5, 2025
6. **A Note on Adaptive Security in Hierarchical Identity-Based Encryption**
   with Rishab Goyal and Venkata Koppula
   45th Annual International Cryptology Conference, CRYPTO 2025
7. **Non-Committing Identity Based Encryption: Constructions and Applications**
   with Rishab Goyal, Fuyuki Kitagawa, Venkata Koppula, Ryo Nishimaki and Takashi Yamakawa
   28th IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2025
8. **Incompressible Functional Encryption**
   with Rishab Goyal, Venkata Koppula and Aman Verma
   16th Innovations in Theoretical Computer Science, ITCS 2025
9. **Leakage-Resilient Key-Dependent Message Secure Encryption Schemes**
   with Dhairya Gupta and Harihar Swaminathan
   25th International Conference on Cryptology, INDOCRYPT 2024
10. **Leakage-Resilient Incompressible Cryptography: Constructions and Barriers**
    with Kaartik Bhushan, Rishab Goyal, Venkata Koppula, Varun Narayanan and Manoj Prabhakaran,
    International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2024
11. **Complexity of Monomial Prediction in Cryptography and Machine Learning**
    with Pranjal Dutta and Santanu Sarkar,
    26th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2024
12. **On the Maximum Distance Sublattice Problem and Closest Vector Problem**
    with Rajendra Kumar and Shashank K Mehta,
    26th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2024

13. **Efficient reductions and algorithms for Subset Product**
with Pranjal Dutta,
9^{th} Annual International Conference on Algorithms and Discrete Applied Mathematics, CALDAM 2023
Best Student Presentation Award

14. **On the Variants of Subset Sum: Projected and Unbounded**
with Pranjal Dutta,
25^{th} International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2023

15. **On the bases of $\mathbb{Z}^n$ lattice**
with Shashank K Mehta,
24^{th} International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2022

16. **Weak-keys and key-recovery attack for TinyJAMBU**
with Pranjal Dutta and Santanu Sarkar,
Scientific Reports, Volume 12, Article 16313, 2022

17. **On the hardness of monomial prediction and zero-sum distinguishers for Ascon**
with Pranjal Dutta and Santanu Sarkar,
12^{th} International Workshop on Coding and Cryptography, WCC 2022

18. **Algebraic algorithms for variants of Subset Sum**
with Pranjal Dutta,
8^{th} Annual International Conference on Algorithms and Discrete Applied Mathematics, CALDAM 2022
Best Student Presentation Award

19. **Cryptanalysis of Round-Reduced KECCAK using Non-Linear Structures**
20^{th} International Conference on Cryptology, INDOCRYPT 2019

20. **Cryptanalysis of 1-Round KECCAK**
with Rajendra Kumar and Hoda Al Khzaimi,
10^{th} International Conference on Cryptology, AFRICACRYPT 2018

Papers Under Submission

1. **On the Largest Cardinality Subset Sum**
with Deepak Bhati, Anubhav Dhar, Pranjal Dutta and Karol Węgrzycki
Submitted to STACS 2027
Paper

2. **A Simple Compiler for CCA2-Secure Pseudorandom Codes in the Standard Model**
with Nico Döttling, Antoine Joux, Venkata Koppula and Hendrik Waldner
Paper

3. **Weak Pigeonhole Equal-Sums made Simpler and Faster**
with Deepak Bhati, Pranjal Dutta, Antoine Joux and Karol Węgrzycki

4. **Quantum Pseudorandom Codes**
with Nico Döttling and Anne Müller

Academic Achievements

1. Won the Outstanding Paper award in TCC 2025.
2. Won the Best Student Presentation award (one of the 5 winners) in CALDAM 2023.

3. Won the Best Student Presentation award (one of the 3 winners) in CALDAM 2022.
4. Awarded **Prime Minister's Research Fellowship** in 2018 (received approximately USD 50,000 for a duration of 4 years to cover stipend and other expenses related to research).
5. Awarded Certificate of Merit for Academic Excellence in M.Tech. Computer Science and Engineering at IIT Kanpur, academic year 2016–2017.
6. Secured Rank 28 (Computer Science, Part A) in Joint Entrance Screening Test (JEST-2016).
7. Secured All India Rank 575 in Graduate Aptitude Test in Engineering (GATE 2016)
8. Secured fourth place in the first round of Amrita InCTF 2015.

Short Term Research Visit

1. **National Institute of Technology Calicut** (Aug 2026), Host: Prof. K. Murali Krishnan.
2. **Indian Institute of Space Science and Technology, Trivandrum** (Aug 2026), Host: Prof. Deepak Mishra.
3. **Universidad Carlos III de Madrid, Leganés** (Jun 2026), Host: Prof. Lorena González-Manzano.
4. **University of Warsaw** (Mar 2026).
5. **IMDEA Software Institute** (May 2026), Host: Prof. Dario Fiore
6. **Technical University of Denmark** (Dec 2025), Host: Prof. Christian Majenz
7. **International Institute of Information Technology Hyderabad** (Aug 2024), Host: Dr. Suryajith Chillara
8. **University of Wollongong, Australia** (Apr 2024), AICCTP workshop visit.
9. **Indian Institute of Space Science and Technology, Trivandrum** (Mar 2024), Host: Prof. Deepak Mishra.
10. **Microsoft Research India, Bangalore** (Oct 2023), Host: Satya Lokam.
11. **International Centre for Theoretical Sciences Bangalore** (Oct 2023), Host: Prof. Jaikumar Radhakrishnan
12. **Tata Institute of Fundamental Research, Mumbai** (Jul 2023), Host: Prof. Vinod M. Prabhakaran.
13. **Indian Institute of Technology Bombay** (Jul 2023), Host: Prof. Manoj M. Prabhakaran
14. **Institute of Science and Technology Austria** (Sept 2022), Host: Prof. Krzysztof Pietrzak

Research Internships & Projects

1. Visiting scholar at IIT Delhi hosted by Prof. Venkata Koppula (Feb 2023).
2. Visiting scholar at Microsoft Research India hosted by Satya Lokam (Jun 2018, Oct 2018, Mar 2019, Sept 2019).
3. Visiting scholar at New York University, Abu Dhabi hosted by Prof. Hoda AlKhzaimi (Oct 2017).

Academic Talks and Presentations

1. **Recent Trends in Cryptography**, FSTTCS 2026 workshop, IIT Delhi, 19–20 December 2026. Scheduled speaker (upcoming).
2. **Invited Talk**, National Institute of Technology Calicut, 31 August 2026.
   Title: Limits of Black-Box Constructions of Pseudorandom Codes.
3. **Invited Talk**, IIST, Trivandrum, 18 August 2026.
   Title: Secrets, Quantum and AI.
4. **Invited Talk**, IMDEA Software Institute, Madrid, 25 May 2026.
   Title: Limits of Black-Box Constructions of Pseudorandom Codes.
5. **ITCS Graduating Bits**, Informal Talk.
6. **CRYPTO 2025**, Conference Talk.
   Title: A Note on Adaptive Security in Hierarchical Identity-Based Encryption
7. **PKC 2025**, Conference Talk.
   Title: Non-Committing Identity Based Encryption: Constructions and Applications
8. **ITCS 2025**, Conference Talk.
   Title: Incompressible Functional Encryption
9. **INDOCRYPT 2024**, Conference Talk.
   Title: Leakage-Resilient Key-Dependent Message Secure Encryption Schemes
10. **SYNASC 2024**, Conference Talk.
    Title: Complexity of Monomial Prediction in Cryptography and Machine Learning
11. **SYNASC 2024**, Conference Talk.
    Title: On the Maximum Distance Sublattice Problem and Closest Vector Problem
12. **Invited Talk**, IIT Delhi, 2024.
    Title: Leakage-Resilience meets Incompressibility.
13. **Continuing Education Programme**, Centre for Railway Information Systems employees, IIT Delhi, 2024. Guest lecture.
14. **Invited Talk**, CSTAR, IIIT Hyderabad, 7 August 2024.
    Title: Leakage-Resilience meets Incompressibility
15. **Invited Talk**, University of Wollongong, Australia, 3 April 2024.
    Title: Incompressible Encryption beyond Public Key Encryption
16. **Invited Talk**, IIST, Trivandrum, 14 March 2024.
    Title: Incompressible Encryption beyond Public Key Encryption
17. **Invited Talk**, Microsoft Research, Bangalore, 27 October 2023.
    Title: Incompressible Encryption beyond Public Key Encryption
18. **SYNASC 2023**, Conference Talk.
    Title: On the Variants of Subset Sum: Projected and Unbounded
19. **Invited Talk**, Trust Lab, IIT Bombay, 12 July 2023 (online).
    Title: Incompressible Encryption
20. **CALDAM 2023**, Conference Talk.
    Title: Efficient reductions and algorithms for Subset Product
21. **SYNASC 2022**, Conference Talk.
    Title: On the bases of $\mathbb{Z}^n$ lattice
22. **SIGTACS**, CSE, IIT Kanpur.
    Title: On the hardness of monomial prediction problem.

23. **STEM Mentorship Program for High School Girl Students**, IIT Delhi, 2023.
    Title: Cryptography: Performing a Task Securely.
24. **Invited Talk**, CSE, IUST Jammu & Kashmir, 2022.
    Title: On the Subset Sum Problem.
25. **SIGTACS**, CSE, IIT Kanpur.
    Title: An Algebraic Algorithm for Hamming Subset-Sum Problem.
26. **WCC 2022**, Workshop Talk.
    Title: On the hardness of monomial prediction problem.
27. **Invited Talk**, PMRF Symposium, 2022.
    Title: Cryptanalysis of KECCAK & Algorithms for Lattice Problems.
28. **SIGTACS**, CSE, IIT Kanpur.
    Title: Cryptanalysis of Round-Reduced KECCAK using Non-linear Structures.
29. **INDOCRYPT 2019**, Conference Talk.
    Title: Cryptanalysis of Round-Reduced KECCAK using Non-Linear Structures.
30. **SIGTACS**, CSE, IIT Kanpur.
    Title: Leftover Hash Lemma
31. **SIGTACS**, CSE, IIT Kanpur.
    Title: Lattices in Computer Science
32. **SIGTACS**, CSE, IIT Kanpur.
    Title: A Deterministic Exponential Time Algorithm for some lattice problems

Teaching Experience

1. 1000-2M26QC – Quantum Computing, University of Warsaw, winter semester 2026–2027. Course coordinator and instructor for lectures, tutorials and laboratory sessions; taught in English (9 ECTS).
2. 1000-2M12KI1 – Cryptography I, University of Warsaw, winter semester 2026–2027. Tutorial instructor for two class groups.
3. 1000-2D21KBF – Cryptography, Blockchain & Fintech, University of Warsaw, 2026–2027. Master's seminar co-coordinated with Prof. Stefan Dziembowski and Prof. Tomasz Michalak; seminar instructor.
4. CRYPTO25 - Cryptography at Saarland University, 2025. Delivered a week-long lecture series on key agreement protocols and public-key encryption.
5. COL100 - Introduction to Computer Science at IITD, 2024. Delivered lectures, designed examinations, and supervised laboratory sessions, covering approximately one-third of the course.
6. COL863 - Algebra and Computation (Topics in TCS) at CSE, IITD, 2024. Delivered a module on lattices, designed assignments, and graded coursework.

Research Mentoring

1. PhD research mentoring:
   (a) Deepak Bhati, CISPA
   (b) Hadi Barzegar, CISPA
   (c) Anne Müller, CISPA
2. Master and dual-degree research mentoring:
   (a) Shankh Gupta, IIT Delhi, dual-degree research, 2024–2025
   (b) Abhinav Kumar, IIT Delhi, 2023–2024 (co-authored paper in Communications in Cryptology, 2025)

(c) Dhairya Gupta, IIT Delhi, 2023–2024 (co-authored paper at INDOCRYPT 2024)

3. Bachelor project co-mentoring:
   (a) Naman Verma, IIT Kanpur, 2018–2019 (with Prof. Shashank K. Mehta).
4. Bachelor projects mentored:
   (a) Anish Banerjee, IIT Delhi, 2024–2025
   (b) Harihar Swaminathan, IIT Delhi, 2023–2024 (co-authored paper in Communications in Cryptology, 2025 and INDOCRYPT 2024)
5. Research interns mentored at IIST, 2024:
   (a) Sundar R, B.Tech. student, IIIT Sri City (NTRU cryptography).
   (b) Aiswarya G Raj, M.Tech. student, CET Trivandrum (adversarial robustness of deep neural networks; co-mentored with Prof. Deepak Mishra).
   (c) Ajay R Nair, M.Tech. student, CET Trivandrum (natural adversarial examples; co-mentored with Prof. Deepak Mishra).

Teaching Assistance

1. COL872 - Special Topics in Cryptography at CSE, IITD, 2023
2. CS961 - Modern Cryptology at Emaster Program, IITK 2023, 2022
3. CS972 - Introduction to Linear Algebra at Emaster Program, IITK 2022
4. Modern Algebra at NPTEL 2021, 2018
5. CS641 - Modern Cryptology at CSE, IITK 2021, 2020, 2019, 2018, 2017
6. CS345 - Algorithms II at CSE, IITK 2018
7. ESO207 - Data Structures and Algorithms at CSE, IITK 2017
8. CS3092D - Operating Systems Laboratory at CSE, NITC 2016

Professional Activities

1. Co-organizer, Recent Trends in Cryptography, FSTTCS 2026 workshop, IIT Delhi, with Prof. Venkata Koppula. Scheduled for 19–20 December 2026 (upcoming).
2. Reviewed papers for INDOCRYPT 2021, MFCS 2023, FSTTCS 2023, Journal of Cryptology, EUROCRYPT 2023, ASIACRYPT 2024, ITCS 2025, EUROCRYPT 2025, PKC 2025, ICALP 2025, CRYPTO 2025, STOC 2026, ICALP 2026, TCC 2026, ASIACRYPT 2026.
3. PhD Defence Committee Member, Saarland University, 19 March 2026. Invited examiner for the doctoral defense of Renas Bacho, evaluated thesis quality and oral examination performance.
4. Part of the Indian team for the Australia–India Cyber and Critical Technology Partnership (AICCTP). The IIT Kanpur–University of Wollongong collaboration studies privacy-enhancing cryptography and cloud-computing standardization.

Volunteer Works

1. Lecture delivered at Continuing Education Programme for employees at Centre For Railway Information Systems, IIT Delhi 2024.
2. Lecture delivered at STEM Mentorship Program for High School Girl Students, IIT Delhi 2023.
3. Volunteer at Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2017.
4. Volunteer at Cybersecurity Awareness Week CSAW 2017.
5. Head Coordinator of Special Interest Group on Theoretical Aspects of Computer Science SIGTACS at IIT Kanpur.

Conference & Workshop Attended (offline)

1. CISPA–MPI–UdS retreat, Trier, Germany, November 2025.
2. 23rd International Conference on Theory of Cryptography, TCC 2025, Aarhus, Denmark.
3. 45th Annual International Cryptology Conference, CRYPTO 2025, Santa Barbara, CA, USA.
4. Cryptography 10 Years Later: Obfuscation, Proof Systems, and Secure Computation at Simons Institute for the Theory of Computing (2025), Berkeley, USA.
5. 28th IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2025, Røros, Norway.
6. 16th Innovations in Theoretical Computer Science Conference, ITCS 2025, Columbia University, New York, USA.
7. 22nd International Conference on Theory of Cryptography, TCC 2024, Milan, Italy.
8. Warsaw IACR Summer School on Post-Quantum Cryptography 2024, Warsaw, Poland.
9. 9th Annual International Conference on Algorithms and Discrete Applied Mathematics, CALDAM 2023, Gandhinagar, India.
10. 24th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2022, Hagenberg, Austria.
11. Quantum Algorithms at Simons Institute for the Theory of Computing (2020), Berkeley, USA.
12. Quantum Cryptanalysis of Post-Quantum Cryptography at Simons Institute for the Theory of Computing (2020), Berkeley, USA.
13. Lattices: Geometry, Algorithms and Hardness at Simons Institute for the Theory of Computing (2020), Berkeley, USA.
14. Secure Multiparty Computation: Theory and Practice workshop held at IISc (2020), Bangalore, India.
15. 20th International Conference on Cryptology, INDOCRYPT 2019, Hyderabad, India.
16. Theory of Cryptography Conference, TCC 2018, Goa, India.
17. 37th Foundations of Software Technology and Theoretical Computer Science 2017, Kanpur, India.

Conference & Workshop Attended (online)

1. 26^{th} International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2024, Timișoara, Romania.
2. 25^{th} International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2023, Nancy, France.
3. 12^{th} International Workshop on Coding and Cryptography, WCC 2022.
4. 8^{th} Annual International Conference on Algorithms and Discrete Applied Mathematics, CALDAM 2022

Referees

1. **Prof. Nico Döttling**
   CISPA Helmholtz
   Email: doettling@cispa.de
2. **Prof. Antoine Joux**
   CISPA Helmholtz
   Email: joux@cispa.de
3. **Prof. Venkata Koppula**
   Department of CSE, IIT Delhi
   Email: kvenkata@cse.iitd.ac.in
4. **Prof. Manoj Prabhakaran**
   Department of CSE, IIT Bombay
   Email: mp@cse.iitb.ac.in
5. **Prof. Manindra Agrawal**
   Department of CSE, IIT Kanpur
   Email: manindra@cse.iitk.ac.in
6. **Prof. Shashank K Mehta**
   Department of CSE, IIT Kanpur (Retired)
   Email: skmehta@cse.iitk.ac.in